REMARKS/ARGUMENTS

The following remarks are intended to fully respond to the Office Action mailed December 23, 2008, hereinafter "Office Action." In the Office Action, claims 1, 3-16, 18-20, and 22 were examined, and all claims were rejected. More specifically, claims 1, 3-16, 18-20, and 22 were rejected under 35 USC 103(a) as being unpatentable over Hanna et al., US Patent No. 6,801,998 (hereinafter "Hanna") in further view of Huitema et al., US Patent No. 7,068,789 (hereinafter "Huitema").

In this Response, claims 1, 9, and 16 have been amended and no claims have been cancelled or added.

Reconsideration of these rejections, as they might apply to the original and amended claims in view of these remarks, is respectfully requested.

Claim Rejections – 35 USC § 103(a)

The Examiner rejected claims 1, 3-16, 18-20, and 22 under 35 USC § 103(a) and being unpatentable over Hanna in view of Huitema. Applicants respectfully traverse the § 103(a) rejections of claims 1, 3-16, 18-20, and 22 because the Office Action failed to state a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at the time the invention was made. M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424 F.2d 1382, 1385 (C.C.P.A. 1970). Further, under *KSR Int'l Co. v. Teleflex, Inc.*, there "must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." 127 S. Ct. 1727, 1741 (2007). Specifically, the references fail to teach or suggest all of the claimed limitations. More particularly, the cited references fail to teach or suggest, at least, an embedded use policy that expresses a privacy policy providing instructions as to how group identity information may be used, wherein the embedded use policy is stored with the group identity information, as recited in independent claim 1.

Hanna relates to a system for determining whether an applicant is a member of a pre-established, authorized group without providing the applicant the names of the authorized group or groups. The Hanna system comprises a client, an application server, and a group member server. (*See* Hanna, Fig. 1). A client who desires a service that is performed by the application server logs on to the application server and requests the service from it. In response, the application server requests proof from the client that the client is a member of a group that has permission to receive the requested service. (*See id.*, col. 4, l. 64 – col. 5, l. 33). However, the Hanna system is designed such that it avoids providing the client with information about which group or groups are eligible to receive the requested service. Instead, the application server provides the client with an encrypted message intended for a group membership server. (*See id.*, col. 5, ll. 36-62). The client forwards the encrypted message to the applicable group server which decrypts the message to reveal information regarding authorized groups. The group server uses this information to determine whether the client is a member of one of the groups or meets the criteria for membership in one of the specified groups. (*See Id.*, col. 5, l. 62 – col. 7, l. 6). The group server then returns an encrypted message to the application server indicating whether or not the client is a member of a group authorized to receive the requested service. Upon receipt, the application server decrypts the message and determines whether or not to grant the requested service to the client.

However, Hanna does not teach or suggest an embedded use policy that expresses a privacy policy providing instructions as to how group identity information may be used, wherein the embedded use policy is stored with the group identity information. The Office Action alleges that the reference's teaching of encrypted messages teaches this limitation. More specifically, the Office Action argues:

> "Examiner views the "encrypted message" that is provided to the client by the application server as being analogous to the "use policy". The encrypted message is forwarded by the client to the group membership server in order to prove eligibility to receive a requested service. The encrypted message contains information detailing whether the client is a member of the group. Examiner views the as being analogous to "information about a principal". The ability of the encrypted message to prove eligibility within a group is viewed as being analogous to conveying the originators instructions about the uses to which the contents may be put."

Applicants respectfully disagree that the "encrypted message" teaches an embedded use policy that expresses a privacy policy providing instructions as to how group identity information may be used, wherein the embedded use policy is stored with the group identity information. Even if the encrypted message was to constitute a use policy, which Applicants disagree is the case, the reference does not teach that the encrypted message is embedded in a group identity information document. Additionally, the reference does not teach that the encrypted message is stored with the group identity information as is the embedded use policy recited in claim 1.

The Office Action appears to correlate the encrypted message with the embedded use policy because the encrypted message prohibits some entities from viewing the contents of the message, i.e., anyone who does not have the proper key to decrypt the encrypted message. Applicants note that this is not an embedded use policy that expresses a privacy policy, rather the encrypted message is means for securely transmitting a message. Furthermore, as recited in claim 1, the embedded use policy is stored with the group identity information, thus ensuring that the embedded use policy is always applied to the group identity information. On the other hand, once the encrypted message of Hanna is decrypted, there is no guarantee that the information stored in the encrypted message will be protected. For at least the forging reasons, Hanna fails to teach all of the features of claim 1.

Huitema fails to compensate for this deficiency. Huitema relates to "a method for ensuring valid and secure peer-to-peer communications in a group structure. Specifically, the system of the present invention presents a method of ensuring secure peer-to-peer group formation, group member addition, group member eviction, group information distribution, etc." (Huitema, Abstract). The Office Action has failed to show that Huitema teaches or suggests an embedded use policy that expresses a privacy policy providing instructions as to how group identity information may be used, wherein the embedded use policy is stored with the group identity information. Thus, independent claim 1 is allowable over the cited references.

For at least the same reasons, independent claim 9 is also allowable over the cited references. Claim 9 recites, *inter alia*, a group ID generate module generating a group certificate comprising at least a public key, an embedded use policy that expresses a privacy policy providing instructions as to how group identity information may be used, wherein the embedded

use policy is stored with the group identity information, and a digital signature for the group. Thus, for at least the same reasons as noted above, independent claim 9 is also allowable over the cited references.

Independent claim 16 is also allowable over the cited references. Independent claim 16, recites, *inter alia*, generating at the initiating system a group certificate comprising at least a group use policy that expresses a privacy policy providing instructions as to how group identity information may be used, wherein the embedded use policy is stored with the group identity information, a group public key and a digital signature for the group signed with a group private key associated with group public key. Thus for at least the same reasons previously discussed, independent claim 16 is allowable over the cited reference.

Furthermore, independent claim 16 recites a personal use policy that expresses a personal privacy policy providing instructions as to how personal identity information may be used, wherein the embedded personal use policy is stored with the personal identity information. The cited reference also fails to teach the personal use policy.

Finally, the Office Action again summarily rejected claim 16 for the same reasons as claim 1 and simply recites the elements of claim 16. (*See Office Action*, pp. 6-8). In rejecting claim 16, the Office Action points to col. 6 lines 10-14 of Hanna which states "the message may comprise an encrypted certificate signed by the respective group membership server 16 that indicates that the applicant is a member of the specified group. The certificate is signed by the respective group membership server. This encryption key may comprise a shared key or alternatively, the public key of a public key pair maintained by the application server 12." (Office Action, p. 7). However it is unclear how this line renders the following obvious. Applicants disagree that this statement from Hanna teaches or suggests the following features as alleged in the Office Action:

> sending the group certificate to the receiving system to establish the new group identity at the receiving system;
>
> sending a membership certificate to the receiving system to establish the originator as a member of the new group at the receiving system;

generating a personal certificate having at least a public key of the originator, a personal use policy that expresses a personal privacy policy providing instructions as to how personal identity information may be used, wherein the embedded personal use policy is stored with the personal identity information, and a digital signature for the originator signed by the originator with a private key associated with the public key of the originator; and

sending the personal certificate to establish the personal identity of the originator at the receiving system.

Applicants respectfully submit that the Office Action has failed to reject independent claim 16 for its failure to address all of its limitations as previously recited. Applicants respectfully submit that claim 16 is allowable as previously presented.

For the foregoing reasons, the cited references fail to teach or suggest all of the limitations of independent claims 1, 9, and 16 and therefore cannot anticipate or make obvious the present invention as claimed. Claims 1, 9, and 16 are allowable over the recited references of record and should be allowed. All other claims, i.e. claims 3-8, 10-15, 18-21, and 22, depend from one of the allowable independent claims and are, thus, also allowable over the references of record. Therefore Applicants respectfully request that the Examiner issue a notice of allowance for all claims at his earliest convenience.

CONCLUSION

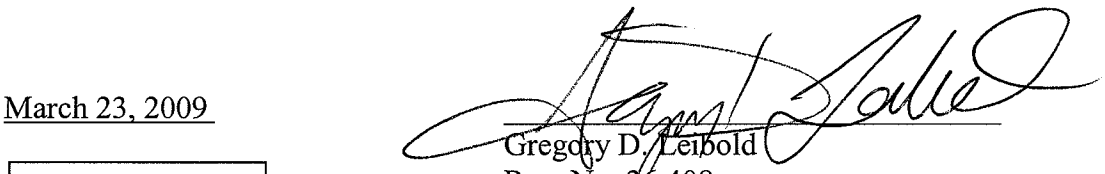
This Amendment fully responds to the Final Office Action mailed on December 23, 2008. Still, that Office Action may contain arguments and rejections that are not directly addressed by this Amendment due to the fact that they are rendered moot in light of the preceding arguments in favor of patentability. Hence, failure of this Amendment to directly address an argument raised in the Office Action should not be taken as an indication that the Applicants believe the argument has merit. Furthermore, the claims of the present application may include other elements, not discussed in this Amendment, which are not shown, taught, or otherwise suggested by the art of record. Accordingly, the preceding arguments in favor of patentability are advanced without prejudice to other bases of patentability.

It is believed that no further fees are due with this Response. However, the Commissioner is hereby authorized to charge any deficiencies or credit any overpayment with respect to this patent application to deposit account number 13-2725.

In light of the above remarks and amendments, it is believed that the application is now in condition for allowance and such action is respectfully requested. Should any additional issues need to be resolved, the Examiner may telephone the undersigned to attempt to resolve those issues.

Respectfully submitted,

Date: March 23, 2009



Gregory D. Leibold
Reg. No. 36,408
MERCHANT & GOULD P.C.
P.O. Box 2903
Minneapolis, Minnesota 55402-0903
303-357-1642